

UNITED STATES PATENT AND TRADEMARK OFFICE
CERTIFICATE OF CORRECTION

PATENT NO. : 6,876,315 B1
DATED : April 5, 2005
INVENTOR(S) : Widmer

Page 1 of 4

It is certified that error appears in the above-identified patent and that said Letters Patent is hereby corrected as shown below:

Title page.

Item [57], **ABSTRACT**,

Line 2, before "format" and after "an" replace "eight-hit" with -- eight-bit --.

Column 7.

Lines 11-12, replace

$$\text{" } a = A \cdot (\bar{A}B \cdot E \cdot F \cdot C \oplus D + \bar{A} \cdot B \cdot C \cdot D \cdot E \oplus F + \bar{A} \cdot B \cdot C \cdot D \cdot E \cdot F) + \text{"}$$
$$\bar{A} \cdot B' \cdot E' \cdot F' \cdot C \oplus D + \bar{A}' \cdot B' \cdot C' \cdot D' \cdot E \oplus F + \bar{A}' \cdot B' \cdot C' \cdot D' \cdot E' \cdot F'$$

with

$$\text{" } a = A \cdot (\bar{A} \cdot B \cdot E \cdot F \cdot C \oplus D + \bar{A} \cdot B \cdot C \cdot D \cdot E \oplus F + \bar{A} \cdot B \cdot C \cdot D \cdot E \cdot F) + \text{"}$$
$$\bar{A}' \cdot B' \cdot E' \cdot F' \cdot C \oplus D + \bar{A}' \cdot B' \cdot C' \cdot D' \cdot E \oplus F + \bar{A}' \cdot B' \cdot C' \cdot D' \cdot E' \cdot F'$$

Column 8.

Line 1, replace

$$\text{" } e = E \cdot (C \cdot D \cdot \bar{E} \cdot F \cdot A \oplus B + A \cdot B \cdot C \cdot D \cdot \bar{E} \cdot F) + C \cdot D \cdot F \cdot A \oplus B + A \cdot B \cdot C \cdot D \cdot F \text{"}$$

with

$$\text{" } e = E \cdot (C \cdot D \cdot \bar{E} \cdot F \cdot A \oplus B + A \cdot B \cdot C \cdot D \cdot \bar{E} \cdot F) + \text{"}$$
$$C' \cdot D' \cdot \bar{E}' \cdot F' \cdot A \oplus B + A' \cdot B' \cdot C' \cdot D' \cdot \bar{E}' \cdot F'$$

Column 10.

Line 26, replace

$$\text{" } e = E \oplus \{ (E \oplus \bar{F}') \cdot (C \oplus D' \cdot D \oplus E' \cdot A \oplus B' \cdot B \oplus C') \} \text{"}$$

with

$$\text{" } e = E \oplus \{ (C \oplus D' \cdot D \oplus \bar{E}' \cdot \bar{E} \oplus F') \cdot \text{"}$$
$$(A \oplus B + A \oplus B' \cdot B \oplus C') \}$$

Line 61, replace " $\bar{a} \cdot b' \cdot e \cdot f \cdot g \cdot h' \cdot c \oplus d + \bar{a}$ "

with -- $\bar{a} \cdot b' \cdot e' \cdot f \cdot g \cdot h' \cdot c \oplus d + \bar{a}$ --.

UNITED STATES PATENT AND TRADEMARK OFFICE
CERTIFICATE OF CORRECTION

PATENT NO. : 6,876,315 B1
 DATED : April 5, 2005
 INVENTOR(S) : Widmer

Page 2 of 4

It is certified that error appears in the above-identified patent and that said Letters Patent is hereby corrected as shown below:

Column 11,

Line 8, replace

“ $n3 = \bar{a} \cdot b' \cdot c' \cdot d \cdot e \cdot f' \cdot g \cdot h' + \bar{a} \cdot b' \cdot e' \cdot f \cdot g \cdot h' \cdot c \oplus d + \bar{a} \cdot b \cdot c' \cdot d' \cdot g \cdot h' \cdot e \oplus f$ ”

with

-- $n3 = \bar{a} \cdot b' \cdot c' \cdot d \cdot e \cdot f' \cdot g \cdot h' + \bar{a} \cdot b' \cdot e' \cdot f \cdot g \cdot h' \cdot c \oplus d + \bar{a} \cdot b \cdot c' \cdot d' \cdot g \cdot h' \cdot e \oplus f$ --

Line 20, replace

“ $B = b \cdot (a \cdot \bar{b} \cdot c' \cdot d' \cdot h' \cdot e \oplus f)' + a' \cdot \bar{b}' \cdot c \cdot d \cdot g \cdot h' \cdot e \oplus f$ ”

with

-- $B = b \cdot (a \cdot \bar{b} \cdot c' \cdot d' \cdot g \cdot h' \cdot e \oplus f)' + a' \cdot \bar{b}' \cdot c \cdot d \cdot g \cdot h' \cdot e \oplus f$ --

Line 33, replace

“ $C = c \cdot (a' \cdot b' \cdot d' \cdot e \cdot f \cdot g \cdot h)' + a \cdot b \cdot d \cdot e' \cdot f' \cdot g \cdot h'$ ”

with

-- $C = c \cdot (a' \cdot b' \cdot d' \cdot e \cdot f \cdot g \cdot h)' + a \cdot b \cdot d \cdot e' \cdot f' \cdot g \cdot h'$ --

Column 12,

Line 14, before “D132” and after “D116,” replace “D1 15,” with -- D115, --.

Lines 26-27, replace

“ $F = f \cdot (c' \cdot d' \cdot \bar{f} \cdot g \cdot h' \cdot a \oplus b + a \cdot b' \cdot e' \cdot \bar{f} \cdot g \cdot h' \cdot c \oplus d)' + +$
 $c \cdot d \cdot e' \cdot \bar{f}' \cdot g \cdot h' \cdot a \oplus b + a' \cdot b \cdot e \cdot \bar{f}' \cdot g \cdot h' \cdot c \oplus d$ ”

with

-- $F = f \cdot (c' \cdot d' \cdot e \cdot \bar{f} \cdot g \cdot h' \cdot a \oplus b + a \cdot b' \cdot e' \cdot \bar{f} \cdot g \cdot h' \cdot c \oplus d)' +$
 $c \cdot d \cdot e' \cdot \bar{f}' \cdot g \cdot h' \cdot a \oplus b + a' \cdot b \cdot e \cdot \bar{f}' \cdot g \cdot h' \cdot c \oplus d$ --

UNITED STATES PATENT AND TRADEMARK OFFICE
CERTIFICATE OF CORRECTION

PATENT NO. : 6,876,315 B1
 DATED : April 5, 2005
 INVENTOR(S) : Widmer

Page 3 of 4

It is certified that error appears in the above-identified patent and that said Letters Patent is hereby corrected as shown below:

Column 12 (cont'd),

Line 33, replace

$$“ n52 = c' \cdot d' \cdot e \cdot \bar{f} \cdot g \cdot h' \cdot a \oplus b + a \cdot b' \cdot e' \cdot f \cdot gh' \cdot c \oplus d ”$$

with

$$“ n52 = c' \cdot d' \cdot e \cdot \bar{f} \cdot g \cdot h' \cdot a \oplus b + a \cdot b' \cdot e' \cdot \bar{f} \cdot g \cdot h' \cdot c \oplus d ”$$

Line 68, replace

$$“ n64 = g \cdot h \cdot e \oplus f + e' \cdot f' \cdot g \oplus h ”$$

with

$$“ n64 = g' \cdot h' \cdot e \oplus f + e' \cdot f' \cdot g \oplus h ”$$

Column 13,

Lines 28-29, replace

$$“ A = a \oplus \{ (e \oplus f \cdot g \cdot h) \cdot (\bar{a} \oplus b \cdot b \oplus c' \cdot c \oplus d \cdot d \oplus e' + \bar{a} \oplus b \cdot b \oplus e' \cdot c \oplus d + \bar{a} \oplus b' \cdot b \oplus c \cdot c \oplus d') \} ”$$

with

$$“ A = a \oplus \{ (e \oplus f \cdot g \cdot h') \cdot (\bar{a} \oplus b \cdot b \oplus c' \cdot c \oplus d \cdot d \oplus e' + \bar{a} \oplus b \cdot b \oplus e' \cdot c \oplus d + \bar{a} \oplus b' \cdot b \oplus c \cdot c \oplus d') \} ”$$

Line 34, replace

$$“ D = d \oplus (a \oplus b \cdot b \oplus c' \cdot c \oplus \bar{d} \cdot \bar{d} \oplus e' \cdot e \oplus f \cdot g \cdot h') ”$$

with

$$“ D = d \oplus (a \oplus b \cdot b \oplus c' \cdot c \oplus \bar{d} \cdot \bar{d} \oplus e' \cdot e \oplus f \cdot g \cdot h') ”$$

UNITED STATES PATENT AND TRADEMARK OFFICE
CERTIFICATE OF CORRECTION

PATENT NO. : 6,876,315 B1
DATED : April 5, 2005
INVENTOR(S) : Widmer

Page 4 of 4

It is certified that error appears in the above-identified patent and that said Letters Patent is hereby corrected as shown below:

Column 13 (cont'd),

Line 42, replace

" $(a \oplus b \cdot c \oplus d' + a \oplus b' \cdot c \oplus d) \cdot (e \oplus f \cdot g \cdot h' + e \oplus f' "$

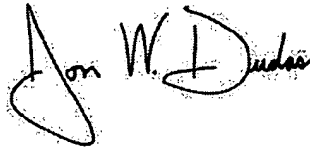
with

-- $(a \oplus b \cdot c \oplus d' + a \oplus b' \cdot c \oplus d) \cdot (e \oplus f \cdot g \oplus h' + e \oplus f' --$

Line 51, after "e.g.," replace "2xfNV" with -- 2xINV --.

Signed and Sealed this

Thirteenth Day of September, 2005



JON W. DUDAS
Director of the United States Patent and Trademark Office